GRZEGORZ LIBOR | Uniwersytet Śląski
w Katowicach

Testowanie w społeczeństwie ryzyka

Abstract: Grzegorz Libor makes an analysis of the notion of the society of risk, extremely trendy today. The researcher concentrates on a technological dangers of a digital world. Grzegorz Libor defines the practice of testing as an argument guaranteeing minimization of fears and tensions evoked by the usage of specialized technical tools and computer programmes. The text clearly explains the strategies of testing , including an invaluable role of a tester, enabling the reduction of stress and curbing a computer chaos in a globalised world.

Key words: sociology, risk, testing games and programmes, tester, society

> Jakość to doskonałość, której nie da się osiągnąć, lecz do której trzeba uporczywie zdążać.
>
> Lao Tsu

Współczesne społeczeństwa nie tylko ze względu na swą złożoność, lecz także zachodzące w nich przemiany definiowane są bardzo często w różnoraki sposób, w zależności od tego, co jest punktem wyjścia lub też kryterium ich wyodrębnienia. Stąd też w literaturze przedmiotu spotkać można takie określenia jak np.: społeczeństwo późnej nowoczesności, społeczeństwo ponowoczesne czy też społeczeństwo sieci.

W ostatnich latach równie popularnym stał się termin społeczeństwa ryzyka.

Koncepcja społeczeństwa ryzyka

Pojęcie ryzyka zyskało swą popularność w dzisiejszej socjologii przede wszystkim dzięki pracom Anthony'ego Giddensa oraz Ulricha Becka.

To właśnie Beck wprowadził pojęcie społeczeństwa ryzyka, które, jego zdaniem, stanowi konsekwencję dwóch zjawisk: indywidualizacji oraz globalizacji. W rezultacie społeczeństwo ryzyka stanowi część tzw. późnej bądź też wysokiej nowoczesności. Wysoka nowoczesność nastała po okresie klasycznej nowoczesności zapoczątkowanej czasem industrializacji – charakteryzującym się podziałami i konfliktami społecznymi, dotyczącymi kwestii produkcji i dystrybucji dóbr społecznych. W społeczeństwie nowego typu natomiast najważniejszą kwestią jest ta, dotycząca radzenia sobie z szeroko pojętym ryzykiem. Pod pojęciem radzenia sobie z ryzykiem rozumieć należy jego zapobieganie, kontrolę, zarządzanie oraz minimalizowanie jego skutków m.in. konsekwencji skażenia środowiska czy też bezrobocia. Zdaniem Becka, ryzyko stało się centralnym punktem naszych codziennych rozważań i istotą współczesności. Choć ryzyko było częścią ludzkiego życia od zawsze, to dziś przybrało zupełnie nowy kształt i charakter. Ma przede wszystkim wymiar zewnętrzny, globalny, a nie, jak do tej pory, wewnętrzny. Ponadto znajduje się poza bezpośrednią kontrolą organów i instytucji państwowych. Pojawienie się zupełnie nowego rodzaju ryzyka wpłynęło nie tylko na sposób funkcjonowania dzisiejszych społeczeństw, lecz także na ich strukturę, tj. podział na klasy, których podstawą wyodrębnienia nie jest, jak do tej pory, własność, ale stopień narażenia na różnego typu zagrożenia. Podobną przemianę przeszły ruchy społeczne, które w swej działalności nawiązują dziś do idei i założeń społeczeństwa ryzyka. Tego typu zjawiska i procesy właściwe są jednak przede wszystkim społeczeństwom zachodnim, które z jednej strony zajęte są zaspokajaniem swych potrzeb materialnych, z drugiej natomiast, zarządzaniem wspomnianym już ryzykiem. Dlatego też problem ryzyka coraz częściej pojawia się w publicznej debacie obok istniejących już od dawna kwestii społecznych. Jego rozwiązanie utrudnia jednak fakt, że zagrożenia charakterystyczne dla współczesnego świata pozbawione są jakichkolwiek granic, nie tylko terytorialnych, lecz także czasowych, co oznacza, że konsekwencje i skutki ich wystąpienia będą odczuwane również przez przyszłe pokolenia. Nie bez znaczenia jest też fakt, że zagrożenia te nie mają charakteru indywidualnego, ale kolektywny – zbiorowy. Dlatego właśnie, zdaniem Giddensa, nowy typ polityki powinien odzwierciedlać nie tylko kwestię tego, w jaki sposób zarządzać ryzykiem, lecz także kwestię przejścia od gospodarki industrialnej, a więc opartej na produkcji, do gospodarki postindustrialnej, której podstawą stały się usługi. Przejściu temu towarzyszy zjawisko migracji inwestycji, produkcji oraz zatrudnienia z regionów o wysokich kosztach pracy do regionów, gdzie koszty te są znacznie niższe. Ponadto proces niespotykanej na taką skalę konsumpcji, powiązany ze zmianą w sposobie życia i wspomnianą już indywidualizacją[1].

Indywidualizację tę rozumieć należy zatem jako konsekwencję zmian w standardzie życia, które doprowadziły do zaniku tożsamości klasowej opartej

[1] Więcej: J. Germov, M. Poole: *Public Sociology: An introduction to Australian Society*. Crows Nest 2007.

na tradycyjnym statusie, a więc, inaczej mówiąc, dywersyfikacji stylów życia. Beck wyróżnia trzy rodzaje tak rozumianej indywidualizacji: 1) dysocjację tradycyjnych więzi oraz zobowiązań klasowych; 2) utratę gwarancji dotyczących wiary, wartości i norm społecznych warunkujących nasze zachowanie; 3) nowy rodzaj zaangażowania społecznego, który charakteryzuje się rosnącą zależnością stylów życia i mechanizmów rynkowych[2].

Indywidualizacji tej towarzyszy zjawisko globalizacji, którego jednym z wymiarów jest właśnie fakt negacji dotychczasowego klasowego charakteru społeczeństw industrialnych. Ryzyka nie da się uniknąć. Nie mogą go uniknąć nawet Ci, którzy stają się jego źródłem, a więc osoby doprowadzające do jego urzeczywistnienia. Prędzej czy później także oni będą musieli zmierzyć się z konsekwencjami zagrożeń, do których pojawienia się przyczynili[3].

Zdaniem Becka, pojawienie się nowego rodzaju zagrożeń i ich sukcesywne umacnianie w naszej rzeczywistości stanowi rezultat niepowodzeń technonaukowej racjonalności. Niepowodzeń, które, wg niego, są cechą wrodzoną późnej nowoczesności. Nauka i technologia, jak pokazuje praktyka, nie są w stanie zagwarantować nam bezpieczeństwa. Paradoks polega jednak na tym, że z jednej strony potrzebujemy nauki coraz bardziej, z drugiej, jest ona coraz mniej skuteczna w pełnieniu roli, jaka została jej przypisana. Krytykując naukę oraz technologię, Beck zwraca jednak uwagę na to, że dziś każdy z nas stał się ekspertem późno nowoczesnego ryzyka. Nauka nie dostarczyła nam bowiem satysfakcjonującej odpowiedzi na pytanie, jak radzić sobie z pojawiającymi się nieustannie w zglobalizowanym świecie zagrożeniami. Beck wprowadza zatem pojęcie modernizacji refleksyjnej, a więc takiej, w której mamy do czynienia z licznymi, niemniej akceptowanymi źródłami wiedzy. Koncepcja Becka neguje w rezultacie istotę jakiejkolwiek ekspertyzy. W ten sposób wszystko staje się przedmiotem polityki przybierającej postać dyskusji jednostek i organizacji prezentujących w omawianym temacie ryzyka odmienną wiedzę i stanowiska. Na potwierdzenie tych słów często przytacza się dane Eurobarometru, z których wynika, że 57% badanych uważa, iż nauka i technologia są odpowiedzialne za większość problemów środowiskowych współczesnego świata[4].

Należy jednak mieć na uwadze fakt, że ryzyko rozumiane jest przez nas w różny, czasem bardzo odmienny sposób. W tym miejscu warto sięgnąć do badań Gabe'a Mythena i Sandry Walklate. Jedno z ważniejszych odkryć dotyczących aspektów ryzyka i życia codziennego, było następujące: z jednej strony ludzie świadomi ryzyka podejmowali kroki mające na celu jego uniknięcie, z drugiej natomiast wskazywali, że jego podejmowanie stanowi integralną część naszego

[2] U. Engel, H. Strasser: *Global Risks and Social Inequality: Critical Remarks on the Risk-Society Hypothesis*. "Canadian Journal of Sociology" 1998, No. 1 (23), s. 91–98.

[3] Ibidem.

[4] M. Kearnes: *Spotlight on... Risk Society: Towards a New Modernity by Ulrich Beck*. "Geography" 2008, Vol. 93, s. 122–124.

istnienia oraz nierzadko uwarunkowane jest cechami charakteru. Badani za podejmowanie ryzyka uznawali również uprawianie niebezpiecznych sportów, takich jak surfing czy wspinaczka, ale także decyzję o założeniu rodziny, o zmianie miejsca zamieszkania bądź zaciągnięciu kredytu. Z badań wynika ponadto, że respondenci nadawali ryzyku pozytywne konotacje i znaczenie w trzech przypadkach: 1) kiedy podejmowanie ryzyka postrzegane było jako sposób na poprawę swojej sytuacji życiowej; 2) kiedy pozwalało osiągnąć dodatkowe emocje – gdy uczucie strachu i wszelkie obawy ustępowały miejsca przyszłym, emocjonalnym zyskom; 3) kiedy było sposobem sprawowania kontroli nad własnym ciałem i samym sobą, a także umożliwiało radzenie sobie z negatywnymi emocjami i trudnościami życiowymi. Innymi słowy podejmowanie ryzyka traktowane było jako doskonała odskocznia od codziennych problemów. Dawało bowiem nie tylko poczucie kontroli, lecz także budowało wiarę we własne możliwości[5].

Za odmianę ryzyka respondenci postrzegali także nadużywanie substancji psychoaktywnych, seks bez zabezpieczenia, przestępczość czy też bezdomność[6].

Jak pisze Iain Wilkinson w komentarzu do prac Giddensa i Becka na temat ryzyka: „W przypadku, gdy nasze umysły wypełnione są myślami o ryzyku, wówczas pojawia się w Nas wątpliwość w odniesieniu do naszej osobistej zdolności do życia w bezpieczeństwie. Społeczne znaczenie świadomości ryzyka polega na tym, że świadomość ta ma zdolność koncentracji naszej uwagi na niepokoju i chęci maksymalizacji umiejętności kontroli naszego losu i przeznaczenia; równocześnie, zaczynamy zadawać sobie pytanie, na temat tego, jak powinniśmy żyć i co powinniśmy robić, aby unikać otaczającego Nas niebezpieczeństwa"[7].

Naczelnym hasłem społeczeństwa ryzyka i podstawą więzi łączących jego członków stało się zatem stwierdzenie: „boję się"[8].

Pojęciu społeczeństwa ryzyka towarzyszy jeszcze jedno pojęcie, którego nie sposób pominąć – jest to „państwo regulacyjne" (*regulatory state*), a więc takie, w którym, jak sama nazwa wskazuje, rząd pełni przede wszystkim funkcje regulacyjne, a nie, jak do tej pory, funkcje pracodawcy i właściciela nieruchomości. Państwo regulacyjne stanowi zatem odpowiedź na trudności, a także problemy wynikające z pojawienia się nowego rodzaju i typu zagrożeń. Ryzyko jest w takim przypadku postrzegane jako próba pogodzenia dwóch pozornie sprzecznych idei, tj. idei indywidualizmu oraz idei egalitaryzmu. Z jednej strony bowiem każdy z nas ma własny styl życia i jego wizję, z drugiej jednak, łączymy się w imię solidarności w obliczu pojawiających się i wspólnych niebezpieczeństw. Wyrazem tej solidarności są właśnie wspomniane już regulacje. Po raz pierwszy pojawiać zaczęły się one w świecie finansów. Każdy kolejny kryzys gospodarczy skutkuje występowaniem

[5] G. Mythen, S. Walklate: *Beyond the Risk Society: Critical Reflections on Risk and Human Security*. Maidenhead 2006, s. 20–21.

[6] N.J. Davis: *Youth Crisis: Growing Up in the High-Risk Society*. Westport 1999, s. 24.

[7] I. Wilkinson: *Anxiety in a Risk Society*. New York 2001, s. 103.

[8] J. Adams: *Risk*. London 1995, s. 181.

kolejnych. To samo zjawisko zaobserwować można również w innych dziedzinach naszego życia[9].

Istota i znaczenie procesu testowania

Niniejszy artykuł poświęcony został jednak tylko jednej, wybranej dziedzinie, a więc dziedzinie stosowanego przez nas każdego dnia oprogramowania komputerowego. Wybór takiego, a nie innego, tematu wymaga jednak wyjaśnienia.

W lutym bieżącego roku portal internetowy gadzetomania.pl opublikował listę najsłynniejszych błędów programistycznych. Listę tę otwiera misja na Wenus będąca wspólnym dziełem NASA, JPL oraz USAF o łącznej wartości przekraczającej 18 mln dolarów, która na skutek błędnego zapisu równania, wprowadzającego niewłaściwe trajektoria lotu rakiety, zakończyła się niepowodzeniem. Na drugim miejscu znalazła się usterka kanadyjskiej maszyny do radioterapii nowotworów Therac-25, w której przypadku taka, a nie inna, kombinacja klawiszy powodowała, że pacjent otrzymywał niebezpieczną dla zdrowia i życia dawkę programowania. Błąd ten doprowadził do śmierci 5 osób i do poparzeń u 1 osoby. Jeszcze poważniejsze konsekwencje miała usterka w zegarze systemu obrony przeciwrakietowej Patriot, powodująca śmierć 28 amerykańskich żołnierzy, którzy stacjonowali w jednostce wojskowej w Arabii Saudyjskiej. Z powodu usterki system nie był w stanie prawidłowo lokalizować pojawiającego się zagrożenia. Kolejne miejsce zajął błąd, jaki wystąpił w kolejnej edycji programu europejskiej agencji kosmicznej ESA o nazwie Ariane 5, polegający na przekopiowaniu kodu starego oprogramowania do zupełnie nowej konstrukcji rakiety. Usterka ta kosztowała bagatela 400 mln dolarów! Listę zamyka awaria sieci energetycznej, do której doszło w 2003 roku w Stanach Zjednoczonych i Kanadzie, w której wyniku prądu pozbawionych zostało ponad 50 mln ludzi! Błąd pojawił się w systemie, który odpowiadał za zarządzanie energią i jej przepływem, prowadząc do przeciążenia sieci, a następnie jej uszkodzenia. W rezultacie wiele instytucji nie tylko publicznych, lecz także prywatnych poniosło olbrzymie straty finansowe[10].

Usterki i defekty oprogramowania, stanowiące konsekwencję ludzkich pomyłek i błędów, mogą mieć zatem, jak zaprezentowano na przykładach, nie tylko poważne skutki finansowe, lecz także poważne konsekwencje dla naszego zdrowia i życia. Próbą odpowiedzi na tego typu zagrożenia i wynikające ze stosowania różnego rodzaju oprogramowania ryzyko jest praktyka testowania każdego programu

[9] Ch. Hood, H. Rothstein, R. Baldwin: *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford 2004, s. 4–5.

[10] M. Kamiński: *Najsłynniejsze błędy programistyczne*. http://gadzetomania.pl/2013/02/18/najslynniejsze-bledy-programistyczne-cz-2 (dostęp: 22.05.2013).

zarówno przed, jak i po jego *release*, a więc wypuszczeniu na rynek. Zgodnie z ISTQB[11] ryzyko definiowane jest jako możliwość wystąpienia zdarzenia, niebezpieczeństwa, zagrożenia lub też sytuacji powodującej niepożądane konsekwencje lub potencjalny problem. Poziom ryzyka natomiast to prawdopodobieństwo wystąpienia niekorzystnego zdarzenia oraz jego wpływu.

W testowaniu oprogramowania wyróżnia się dwa rodzaje ryzyka. Pierwszy to ryzyko projektowe, które odnosi się do zdolności projektu do osiągnięcia danego celu. Drugi to ryzyko produktowe związane bezpośrednio z kolei z możliwością wystąpienia awarii.

Ryzyko pierwszego typu tworzą czynniki organizacyjne, techniczne, a także zewnętrzne. Wśród najczęściej pojawiających się problemów wymienia się w tym miejscu m.in. problemy komunikacyjne, problemy kadrowe, jak chociażby niewystarczające umiejętności programistów czy testerów, problemy z dostępem do potrzebnych narzędzi oraz środowiska testowego, a także problemy z dostawcami, którzy bardzo często nie wywiązują się z przyjętych zobowiązań.

Jeśli chodzi z kolei o ryzyko produktowe, wiąże się ono najczęściej z dostarczeniem wadliwego oprogramowania, niską jakością i brakiem spójności danych, niedostatecznymi atrybutami oprogramowania, a także możliwością wyrządzenia szkody użytkownikowi.

Dlatego też w swej istocie testowanie wykorzystywane jest do zredukowania ryzyka, stanowiąc proaktywny sposób zarządzania nim. Ryzyko stanowi zatem jeden z ważniejszych czynników wpływających na sposób planowania testów, a także rodzaj stosowanych narzędzi. Właściwy ich dobór wpływa nie tylko na redukcję powtarzającej się pracy, lecz także na obiektywność oceny, łatwiejszy dostęp do danych o testach i testowaniu oraz na spójność prowadzonych prac testerskich. Wybór odpowiednich narzędzi wiąże się jednak również z pewnym ryzykiem związanym z nierealistycznymi oczekiwaniami co do ich możliwości, kosztów ich implementacji, niedoszacowaniem czasu potrzebnego do osiągnięcia znaczących korzyści, nadmierną wiarą w ich możliwości czy lekceważeniem zależności i problemów w zakresie współpracy z innymi programami czy też systemami.

Do tego wszystkiego dochodzi presja czasu, otoczenia, a także zmieniająca się nieustannie infrastruktura techniczna.

Ryzyko nie ma zatem w tym przypadku charakteru jednostronnego, lecz wielostronny. To z pewnością jedynie utrudnia skuteczne nim zarządzanie, jak też minimalizowanie jego negatywnych konsekwencji.

Tak rozumiane testowanie, a więc z perspektywy ryzyka w kategoriach redukcjonistycznych, aby realizować we właściwy sposób powierzone mu zadania oraz funkcje, musi opierać się na solidnych podstawach, które najczęściej przyjmują postać określonych standardów oraz podstaw prawnych.

---

[11] Foundation Level Syllabus. http://www.istqb.org/downloads/syllabi/foundation-level-syllabus.html (dostęp: 20.05.2013).

Nie sposób jednak wymienić wszystkich standardów obowiązujących współczesnych testerów. Dlatego dalej zaprezentowane zostaną jedynie wybrane, najważniejsze z nich.

Jednym z podstawowych standardów jest *Software Engineering – Software Product Quality ISO 9126*. Oprócz niego wyróżnić można także *Standard for Software Test Documentation – IEEE STD 829-1998*.

Pierwszy składa się z 4 części, tj. modelu jakości, zewnętrznych metryk, wewnętrznych metryk oraz jakości samych metryk. Pod pojęciem modelu jakości rozumieć należy nie tylko jakość zewnętrzną danego oprogramowania czy też aplikacji, lecz także jakość wewnętrzną. Do jakości tych zaliczyć należy: funkcjonalność, niezawodność, łatwość użycia, wydajność, łatwość konserwacji, a także tzw. przenośność. Siłą rzeczy jakości te mierzone są za pomocą odpowiednich metryk, analogicznie zewnętrznych i wewnętrznych, które pokazują, w jakim stopniu dany program czy też system wykonuje poszczególne funkcje oraz zadania. Oprócz wymienionych wspomnieć należałoby również o istnieniu jakości właściwych procesowi użytkowania, do których zalicza się: efektywność, produktywność, satysfakcję użytkownika oraz bezpieczeństwo pracy. Jakości te, jak już wspomniano, są weryfikowane za pomocą różnorodnych metryk. W przypadku metryk wewnętrznych opisywany standard wyróżnia 79 różnego ich typu skierowanych do różnego rodzaju adresatów. Podobnie rzecz ma się w przypadku metryk zewnętrznych, gdzie *Software Engineering – Software Product Quality ISO 9126* podaje jeszcze więcej, bo aż 89 przykładów.

Standard for Software Test Documentation – IEEE STD 829-1998, a więc kolejny z omawianych standardów, definiuje zestaw dokumentów przydatnych, choć niewymaganych, w procesie testowania. Ich wykorzystanie jednak pozytywnie wpływa nie tylko na jakość testowania, lecz także na sposób zarządzania ryzykiem, minimalizowania szans i możliwości jego wystąpienia. Są to następujące dokumenty: Master Test Plan, Level Test Plan, Level Test Design, Level Test Case, Level Test Procedure, Level Test Log, Anomaly Report, Level Interim Test Status Report, Level Test Report oraz Master Test Report. Nieoceniony jest również wkład omawianego standardu w systematyzację najważniejszych pojęć oraz definicji związanych z testowaniem.

Tak rozumiana standaryzacja stanowi jeden ze sposobów budowania zaufania do otrzymywanego przez nas produktu i pełnionych przez niego funkcji oraz posiadanych właściwości. Standaryzacja znajduje jednak zastosowanie w różnych dziedzinach codziennego życia, nie tylko w przypadku omawianej w niniejszym artykule problematyki oprogramowania komputerowego. Stała się ona tak powszechna, że dziś bardzo często dokonując zakupów, nie zwracamy na nią uwagi. Jeszcze niedawno znak jakości ISO stanowił potężny argument zachęcający do wyboru danego produktu oraz rezygnacji z produktu oferowanego przez konkurencję.

Testowanie wymaga również odpowiedniego podejścia samego managementu, a także osób przeprowadzających testy, które stają dziś przed kilkoma wyzwaniami,

w tym przed: 1) potrzebą realizacji szkoleń z zakresu testowania; 2) potrzebą budowania dobrych i właściwych relacji z development; 3) potrzebą testowania przy użyciu specjalistycznych narzędzi; 4) potrzebę tłumaczenia managementowi istoty i znaczenia testowania; 5) potrzebą nieustannego rozmawiania z klientami i użytkownikami danego oprogramowania; 6) potrzebą dysponowania wystarczającą ilością czasu dedykowanego testowaniu; 7) potrzebą współpracy programistów i testerów; 8) potrzebą łączenia czynności testerskich z czynnościami, których celem jest usunięcie znalezionych defektów czy też usterek; 9) potrzebą określenia poziomu jakości, który uznać można by za w pełni satysfakcjonujący oraz zadawalający; 10) potrzebą wprowadzenia bardziej asertywnego podejścia samych testerów, którzy często obawiają się wyrażać swoje negatywne opinie odnośnie jakości testowanej jednostki[12].

Jednym z elementów tejże jakości jest właśnie bezpieczeństwo użytkowania danego programu. Bezpieczeństwo stanowi synonim jakości, gwarancję tego, że korzystając z danej aplikacji, nie znajdziemy się w sytuacji zagrożenia naszego zdrowia lub życia.

Konieczność radzenia sobie z tego typu ryzykiem niesie ze sobą jednak również poważne skutki oraz konsekwencje dla pracy samego testera. Na nim bowiem po części spoczywa odpowiedzialność za to, czy dane oprogramowanie, czy też system spełniają wynikające z wymienionych standardów wymagania, w tym te odnoszące się do szeroko rozumianego pojęcia bezpieczeństwa. Testerzy znajdują się zatem nieustannie pod presją, która jednak nie wynika tylko i wyłącznie ze wspomnianej już odpowiedzialności za jakość produktu, lecz także z presji czasu oraz otoczenia, w tym managementu. Z jednej strony zatem zadanie testerów stanowi odnajdywanie jak największej liczby defektów i usterek, z drugiej strony natomiast sami narażeni są na ich popełnianie. Dlatego też testowaniem danej jednostki rzadko zajmuje się tylko jedna osoba, z reguły jest to grupa testerów. W takim przypadku jednak pojawia się ryzyko wystąpienia zjawiska określanego w psychologii społecznej jako rozproszenie odpowiedzialności: „Kiedy jesteśmy wśród ludzi, zakładamy, że odpowiedzialność za to, co wokół się dzieje, nie spoczywa na nas, lecz dzielą ją wszyscy świadkowie zdarzenia. Myślimy, że na pewno są obok nas osoby bardziej kompetentne, lepiej zorientowane, a wreszcie bardziej niż my zobligowane do działania, np. z racji wieku lub płci. Rozproszenie odpowiedzialności nie tylko blokuje dobre chęci, lecz także skutecznie ucisza nasze sumienie – zawsze możemy powiedzieć »nie tylko ja tam byłem«"[13].

Podobnie rzecz ma się w przypadku testowania, kiedy istnieje ryzyko wystąpienia sytuacji przerzucania odpowiedzialności za nieznalezienie usterek wynikających z błędów popełnionych przez programistów na innych członków zespołu testerskiego. Aby uniknąć tego typu sytuacji w pracy testerów wprowadzono

[12] Ch. Ashbacher: *Surviving the Top Ten Challenges of Software Testing: A People-Oriented Approach*. "Mathematics and Computer Education" 2000, No. 1 (34), s. 92–95.

[13] M. Najda, T. Romer: *Etyka dla sędziów. Rozważania*. Warszawa 2007, s. 104.

swoisty kodeks etyczny, który zakłada, że *deliverables*, a więc produkty dostarczone klientowi spełniać będą najwyższe standardy zawodowe, kierownicy testów natomiast postępować będą w sposób etyczny, promując tego typu podejście także wśród członków ich zespołu. Z kolei zespół za nadrzędne wartości uznawać będzie przede wszystkim uczciwość i niezależność testów, a także działanie zgodnie z najlepiej pojmowanym interesem klientów i pracodawców, ale również interesem publicznym. Ponadto testerzy przez swoją pracę będą dbać o reputację zawodu testera oraz o samodoskonalenie.

Jeszcze innym instrumentem radzenia sobie z ryzykiem jest wybór odpowiedniej strategii komunikowania – takiej, która opiera się na szeroko pojętej współpracy, neutralności przekazu, zrozumieniu argumentów i stanowiska drugiej strony, a także byciu zrozumiałym dla innych.

Strategia ta sprawia, że przekaz jest nie tylko jasny i precyzyjny, lecz także pozbawiony negatywnych emocji. W rezultacie testerzy nie obawiają się przekazywać sobie nawzajem, a także managementowi informacji i komunikatów na temat pojawiających się problemów. Oparte na otwartości oraz rzetelności relacje pozytywnie wpływają na jakość realizowanych testów, a tym samym na jakość wypuszczanego oprogramowania.

Rekapitulując dotychczasowe rozważania, jeden z przejawów tzw. społeczeństwa ryzyka stanowi niewątpliwie fakt, iż obecnie każdy z nas narażony jest na niebezpieczeństwa i zagrożenia wynikające ze stosowania różnego typu systemów, a także różnego rodzaju aplikacji. Jak pokazano, defekty i usterki znajdujące się w oprogramowaniu mogą bowiem doprowadzić do awarii, które stanowić mogą poważne zagrożenie dla naszego zdrowia i życia. Wyjściem z sytuacji napięcia i obawy przed możliwym zagrożeniem, a zarazem gwarancją minimalizacji szans jego wystąpienia, jest omawiana w niniejszym artykule praktyka testowania programów przed ich wypuszczeniem na rynek. Oparta na standardach, uzupełniona kodeksem etycznym, a także wyborem odpowiedniej strategii komunikacyjnej budzi ona zaufanie do produktu czy też usługi, którą wykorzystujemy czy to w celach zawodowych, czy też w życiu prywatnym. Czasem bywa i tak, że jesteśmy zdani na posługiwanie się różnego typu systemami czy tego chcemy, czy też nie. W większości dziedzin naszego życia często nieświadomie, korzystamy bowiem z osiągnięć, rozwoju technologicznego. Nierzadko osiągnięcia te nie tylko chronią nasze życie, lecz także je ratują. Mogą być zatem zarówno zbawieniem, jak i przekleństwem w zależności od tego, czemu służą oraz jak służą. Z tej perspektywy praca testera nabiera w społeczeństwie ryzyka szczególnego znaczenia. To on w znacznej mierze decyduje bowiem, o tym, w jakim stopniu ryzyko wpływa na nasze życie, a w jakim nie. Społeczną rolę testera trudno zatem zanegować czy podważyć. Ze względu na swe znaczenie wymaga ona jednak dalszych badań i analiz.

Literatura

Adams J.: *Risk*. London 1995.
Ashbacher Ch.: *Surviving the Top Ten Challenges of Software Testing: A People-Oriented Approach*. "Mathematics and Computer Education" 2000, No. 1 (34).
Davis N.J.: *Youth Crisis: Growing Up in the High-Risk Society*. Westport 1999.
Engel U., Strasser H.: *Global Risks and Social Inequality: Critical Remarks on the Risk-Society Hypothesis*. "Canadian Journal of Sociology" 1998, No. 1 (23).
Germov J., Poole M.: *Public Sociology: An introduction to Australian Society*. Crows Nest 2007.
Hood Ch., Rothstein H., Baldwin R.: *The Government of Risk: Understanding Risk Regulation Regimes.* Oxford 2004.
Kearnes M.: *Spotlight on... Risk Society: Towards a New Modernity by Ulrich Beck*. "Geography" 2008, Vol. 93.
Mythen G., Walklate S.: *Beyond the Risk Society: Critical Reflections on Risk and Human Security*. Maidenhead 2006.
Najda M., Romer T.: *Etyka dla sędziów. Rozważania*. Warszawa 2007.
Wilkinson I.: *Anxiety in a Risk Society.* New York 2001.

Źródła internetowe

Foundation Level Syllabus. www.istqb.org/downloads/syllabi/foundation-level-syllabus.html (dostęp: 20.05.2013).
Kamiński M.: *Najsłynniejsze błędy programistyczne*. http://gadzetomania.pl/2013/02/18/najslynniejsze-bledy-programistyczne-cz-2 (dostęp: 22.05.2013).